

CLAIMS

What is claimed is:

1. A method of auditing a communication session between a source connected to a first node of a service network and a destination connected to a second node of the service network, the method comprising:

(a) capturing flow activity of selected traffic between the source and the destination at selected states and points in time during the communication session, including:

(i) a flow descriptor for selected datagrams placed in the service network, and

(ii) a service identifier for the selected datagrams which identifies a service interface in the service network that the datagram is transmitted to or received from; and

(b) identifying the service being provisioned on predefined service interfaces; and

(c) using the identified provisioned service and the service identifiers to determine the service provisioned for the datagrams associated with the captured flow activity.

2. The method of claim 1 further comprising:

(d) using the flow descriptors and their time data to identify ingress and egress flow activity that corresponds to each other; and

(e) comparing the services provisioned for the corresponding entries to determine if datagrams transmitted into the service network were provisioned to receive a similar service as datagrams received from the service network.

3. The method of claim 2 wherein a single flow collector captures the ingress and egress flow activity records at a service interface in the service network, and steps (d) and (e) are performed using the flow activity record entries in the single flow collector.

4. The method of claim 2 wherein a first flow collector captures egress flow activity records at a first service interface in the service network, and a second flow collector captures ingress flow activity records at a second service interface in the service network, and steps (d) and (e) are performed using the flow activity record entries in the second and first flow collectors that correspond to each other.

5. The method of claim 1 further comprising:

(d) storing the flow activity in time-stamped flow activity records in at least one flow collector.

6. The method of claim 1 wherein step (a) is performed by a flow meter.

7. The method of claim 1 wherein the service network is a dynamic service network which continuously creates a service resource allocation audit that specifies the service being provided on interfaces of the service network at selected periods of time, wherein step (c) further comprises using portions of the audit having time data which is correlatable to the flow activity to determine the service provisioned for the datagrams associated with the captured flow activity.

8. The method of claim 1 wherein the service network is a non-dynamic service network and a configuration file stores the service being provided on interfaces of the service network, wherein step (c) further comprises using the data in the configuration file to determine the service provisioned for the datagrams associated with the captured flow activity.

9. The method of claim 1 further comprising:

(d) storing in a memory an expected service to be provisioned for the traffic between the source and the destination; and

(e) in a comparator, comparing the service determined in step (c) to be provisioned for the datagrams with the expected service to be provisioned stored in the memory to determine if the expected service was provisioned.

10. The method of claim 1 wherein the service identifier references a security service or a performance service.

11. The method of claim 1 wherein the service network is a virtual private network.

12. The method of claim 1 wherein the service network is an asynchronous transfer mode (ATM) network.

13. The method of claim 1 wherein the service network is a virtual local area network (VLAN).

14. The method of claim 1 wherein the service network is a label switched path (LSP) network.

15. The method of claim 1 wherein the service network is a Layer 2 or Layer 3 network, and the service identifier is a physical interface identifier.

16. A method of auditing a communication session between a source connected to a first node of a service network and a destination connected to a second node of the service network, the method comprising:

(a) capturing flow activity of selected traffic between the source and the destination at selected states and points in time during the communication session, including:

(i) a flow descriptor for selected datagrams placed in the service network, and

(ii) any service labels that are within or appended to the selected datagrams, the service labels referencing the service to be given to the datagram;

(b) identifying a provisioned service being referenced by the service label; and

(c) using the identified provisioned service and the service labels of the captured flow activity to determine the services provisioned for the datagrams associated with the captured flow activity.

17. The method of claim 16 further comprising:

(d) storing the flow activity in time-stamped flow activity records in at least one flow collector.

18. The method of claim 16 wherein the flow activity is captured at a plurality of locations in or at interfaces of the service network, the method further comprising:

(d) using the flow descriptors and their time data to identify flow activity that correspond to each other; and

(e) comparing the provisioned service for the corresponding entries to determine if the datagrams associated with the flow activity were provisioned to receive a similar service.

19. The method of claim 16 wherein the specified service is a security service or a performance service.

20. The method of claim 16 wherein step (a) is performed by a flow meter.

21. The method of claim 16 wherein the flow activity is captured in or at the interface of the service network, the method further comprising:

(d) storing in a memory an expected service to be provisioned for the traffic between the source and the destination; and

(e) in a comparator, comparing the service determined in step (c) to be provisioned for the datagrams with the expected service to be provisioned stored in the memory to determine if the expected service was provisioned.

22. The method of claim 16 wherein a service label lookup facility stores the service labels used by the service network and the provisioned service being referenced by the service label, wherein step (c) further comprises using the service labels captured in the flow activity and the data in the service label file to determine the services provisioned for the datagrams associated with the captured flow activity.

23. The method of claim 16 wherein the absence of any service labels in selected flow activity indicates that no service or a default service was provisioned for the datagrams associated with the flow activity.

24. The method of claim 16 wherein the service network is a virtual private network (VPN).

25. The method of claim 16 wherein the service label is a DiffServ code point within the datagram that indicates the service requirements for the datagram.

26. The method of claim 16 wherein the service label is at least one MPLS label prepended to the datagram.

27. The method of claim 16 wherein the service label is an 802.1Q VLAN identifier prepended to the datagram.

28. The method of claim 16 wherein the service label is an IPSec security payload identifier.

29. The method of claim 16 wherein the service label is an Ipv6 flow identifier.

30. The method of claim 16 wherein the service label is the source and/or destination address of the datagram.

31. The method of claim 16 wherein the service label is the destination service access port (DSAP).

32. The method of claim 16 wherein the service label is the universal resource identifier (URI).

34. The method of claim 16 wherein the service label is application label data.